- in welchen Fällen die Zonen zu segmentieren sind und in welchen Fällen Benutzendengruppen bzw. Mandanten und Mandantinnen logisch oder sogar physisch zu trennen sind,
- welche Kommunikationsbeziehungen und welche Netz- und Anwendungsprotokolle jeweils zugelassen werden,
- wie der Datenverkehr für Administration und Überwachung netztechnisch zu trennen ist,
- welche institutionsinterne, standortübergreifende Kommunikation (WAN, Funknetze) erlaubt und welche Verschlüsselung im WAN, LAN oder auf Funkstrecken erforderlich ist sowie
- welche institutionsübergreifende Kommunikation zugelassen ist.

Die Richtlinie MUSS allen im Bereich Netzdesign zuständigen Mitarbeitenden bekannt sein. Sie MUSS zudem grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies dokumentiert und mit dem oder der verantwortlichen ISB abgestimmt werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

NET.1.1.A2 Dokumentation des Netzes (B) [IT-Betrieb]

Es MUSS eine vollständige Dokumentation des Netzes erstellt werden. Sie MUSS einen Netzplan beinhalten. Die Dokumentation MUSS nachhaltig gepflegt werden. Die initiale Ist-Aufnahme, einschließlich der Netzperformance, sowie alle durchgeführten Änderungen im Netz MÜSSEN in der Dokumentation enthalten sein. Die logische Struktur des Netzes MUSS dokumentiert werden, insbesondere, wie die Subnetze zugeordnet und wie das Netz zoniert und segmentiert wird.

NET.1.1.A3 Anforderungsspezifikation für das Netz (B)

Ausgehend von der Sicherheitsrichtlinie für das Netz MUSS eine Anforderungsspezifikation erstellt werden. Diese MUSS nachhaltig gepflegt werden. Aus den Anforderungen MÜSSEN sich alle wesentlichen Elemente für Netzarchitektur und -design ableiten lassen.

NET.1.1.A4 Netztrennung in Zonen (B)

Das Gesamtnetz MUSS mindestens in folgende drei Zonen physisch separiert sein: internes Netz, demilitarisierte Zone (DMZ) und Außenanbindungen (inklusive Internetanbindung sowie Anbindung an andere nicht vertrauenswürdige Netze). Die Zonenübergänge MÜSSEN durch eine Firewall abgesichert werden. Diese Kontrolle MUSS dem Prinzip der lokalen Kommunikation folgen, sodass von Firewalls ausschließlich erlaubte Kommunikation weitergeleitet wird (Allowlist).

Nicht vertrauenswürdige Netze (z. B. Internet) und vertrauenswürdige Netze (z. B. Intranet) MÜSSEN mindestens durch eine zweistufige Firewall-Struktur, bestehend aus zustandsbehafteten Paketfiltern (Firewall), getrennt werden. Um Internet und externe DMZ netztechnisch zu trennen, MUSS mindestens ein zustandsbehafteter Paketfilter eingesetzt werden.

In der zweistufigen Firewall-Architektur MUSS jeder ein- und ausgehende Datenverkehr durch den äußeren Paketfilter bzw. den internen Paketfilter kontrolliert und gefiltert werden.

Eine P-A-P-Struktur, die aus Paketfilter, Application-Layer-Gateway bzw. Sicherheits-Proxies und Paketfilter besteht, MUSS immer realisiert werden, wenn die Sicherheitsrichtlinie oder die Anforderungsspezifikation dies fordern.

NET.1.1.A5 Client-Server-Segmentierung (B)

Clients und Server MÜSSEN in unterschiedlichen Netzsegmenten platziert werden. Die Kommunikation zwischen diesen Netzsegmenten MUSS mindestens durch einen zustandsbehafteten Paketfilter kontrolliert werden.

Es SOLLTE beachtet werden, dass mögliche Ausnahmen, die es erlauben, Clients und Server in einem gemeinsamen Netzsegment zu positionieren, in den entsprechenden anwendungs- und systemspezifischen Bausteinen geregelt werden.

Für Gastzugänge und für Netzbereiche, in denen keine ausreichende interne Kontrolle über die Endgeräte gegeben ist, MÜSSEN dedizierte Netzsegmente eingerichtet werden.

NET.1.1.A6 Endgeräte-Segmentierung im internen Netz (B)

Es DÜRFEN NUR Endgeräte in einem Netzsegment positioniert werden, die einem ähnlichen Sicherheitsniveau entsprechen.

NET.1.1.A7 Absicherung von schützenswerten Informationen (B)

Schützenswerte Informationen MÜSSEN über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente (z. B. innerhalb des Managementnetzes) kommuniziert wird. Können solche Protokolle nicht genutzt werden, MUSS nach Stand der Technik angemessen verschlüsselt und authentisiert werden (siehe NET.3.3 *VPN).*

NET.1.1.A8 Grundlegende Absicherung des Internetzugangs (B)

Der Internetverkehr MUSS über die Firewall-Struktur geführt werden (siehe NET.1.1.A4 *Netztrennung in Zonen*). Die Datenflüsse MÜSSEN durch die Firewall-Struktur auf die benötigten Protokolle und Kommunikationsbeziehungen eingeschränkt werden.

NET.1.1.A9 Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen (B)

Für jedes Netz MUSS festgelegt werden, inwieweit es als vertrauenswürdig einzustufen ist. Netze, die nicht vertrauenswürdig sind, MÜSSEN wie das Internet behandelt und entsprechend abgesichert werden.

NET.1.1.A10 DMZ-Segmentierung für Zugriffe aus dem Internet (B)

Die Firewall-Strukur MUSS für alle Dienste bzw. Anwendungen, die aus dem Internet erreichbar sind, um eine sogenannte externe DMZ ergänzt werden. Es SOLLTE ein Konzept zur DMZ-Segmentierung erstellt werden, das die Sicherheitsrichtlinie und die Anforderungsspezifikation nachvollziehbar umsetzt. Abhängig vom Sicherheitsniveau der IT-Systeme MÜSSEN die DMZ-Segmente weitergehend unterteilt werden. Eine externe DMZ MUSS am äußeren Paketfilter angeschlossen werden.

NET.1.1.A11 Absicherung eingehender Kommunikation vom Internet in das interne Netz (B)

Ein IP-basierter Zugriff auf das interne Netz MUSS über einen sicheren Kommunikationskanal erfolgen. Der Zugriff MUSS auf vertrauenswürdige IT-Systeme und Benutzende beschränkt werden (siehe NET.3.3 *VPN*). Derartige VPN-Gateways SOLLTEN in einer externen DMZ platziert werden. Es SOLLTE beachtet werden, dass hinreichend gehärtete VPN-Gateways direkt aus dem Internet erreichbar sein können. Die über das VPN-Gateway authentisierten Zugriffe ins interne Netz MÜSSEN mindestens die interne Firewall durchlaufen.

IT-Systeme DÜRFEN NICHT via Internet oder externer DMZ auf das interne Netz zugreifen. Es SOLLTE beachtet werden, dass etwaige Ausnahmen zu dieser Anforderung in den entsprechenden anwendungs- und systemspezifischen Bausteinen geregelt werden.

NET.1.1.A12 Absicherung ausgehender interner Kommunikation zum Internet (B)

Ausgehende Kommunikation aus dem internen Netz zum Internet MUSS an einem Sicherheits-Proxy entkoppelt werden. Die Entkoppelung MUSS außerhalb des internen Netzes erfolgen. Wird eine P-A-P-Struktur eingesetzt, SOLLTE die ausgehende Kommunikation immer durch die Sicherheits-Proxies der P-A-P-Struktur entkoppelt werden.

NET.1.1.A13 Netzplanung (B)

Jede Netzimplementierung MUSS geeignet, vollständig und nachvollziehbar geplant werden. Dabei MÜSSEN die Sicherheitsrichtlinie sowie die Anforderungsspezifikation beachtet werden. Darüber hinaus MÜSSEN in der Planung mindestens die folgenden Punkte bedarfsgerecht berücksichtigt werden:

- Anbindung von Internet und, sofern vorhanden, Standortnetz und Extranet,
- Topologie des Gesamtnetzes und der Netzbereiche, d. h. Zonen und Netzsegmente,
- Dimensionierung und Redundanz der Netz- und Sicherheitskomponenten, Übertragungsstrecken und Außenanbindungen,

- zu nutzende Protokolle und deren grundsätzliche Konfiguration und Adressierung, insbesondere IPv4/IPv6-Subnetze von Endgerätegruppen sowie
- Administration und Überwachung (siehe NET.1.2 *Netzmanagement*).

Die Netzplanung MUSS regelmäßig überprüft werden.

NET.1.1.A14 Umsetzung der Netzplanung (B)

Das geplante Netz MUSS fachgerecht umgesetzt werden. Dies MUSS während der Abnahme geprüft werden.

NET.1.1.A15 Regelmäßiger Soll-Ist-Vergleich (B)

Es MUSS regelmäßig geprüft werden, ob das bestehende Netz dem Soll-Zustand entspricht. Dabei MUSS mindestens geprüft werden, inwieweit es die Sicherheitsrichtlinie und Anforderungsspezifikation erfüllt. Es MUSS auch geprüft werden, inwiefern die umgesetzte Netzstruktur dem aktuellen Stand der Netzplanung entspricht. Dafür MÜSSEN zuständige Personen sowie Prüfkriterien bzw. Vorgaben festgelegt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.1.1.A16 Spezifikation der Netzarchitektur (S)

Auf Basis der Sicherheitsrichtlinie und der Anforderungsspezifikation SOLLTE eine Architektur für die Zonen inklusive internem Netz, DMZ-Bereich und Außenanbindungen entwickelt und nachhaltig gepflegt werden. Dabei SOLLTEN je nach spezifischer Situation der Institution alle relevanten Architekturelemente betrachtet werden, mindestens jedoch:

- Netzarchitektur des internen Netzes mit Festlegungen dazu, wie Netzvirtualisierungstechniken, Layer-2- und Layer-3-Kommunikation sowie Redundanzverfahren einzusetzen sind,
- Netzarchitektur für Außenanbindungen, inklusive Firewall-Architekturen, sowie DMZ- und Extranet-Design und Vorgaben an die Standortkopplung,
- Festlegung, an welchen Stellen des Netzes welche Sicherheitskomponenten wie Firewalls oder IDS/IPS zu platzieren sind und welche Sicherheitsfunktionen diese realisieren müssen,
- Vorgaben für die Netzanbindung der verschiedenen IT-Systeme,
- Netzarchitektur in Virtualisierungs-Hosts, wobei insbesondere Network Virtualization Overlay (NVO) und die Architektur in Vertikal integrierten Systemen (ViS) zu berücksichtigen sind,
- Festlegungen der grundsätzlichen Architektur-Elemente für eine Private Cloud sowie Absicherung der Anbindungen zu Virtual Private Clouds, Hybrid Clouds und Public Clouds sowie
- Architektur zur sicheren Administration und Überwachung der IT-Infrastruktur.

NET.1.1.A17 Spezifikation des Netzdesigns (S)

Basierend auf der Netzarchitektur SOLLTE das Netzdesign für die Zonen inklusive internem Netz, DMZ-Bereich und Außenanbindungen entwickelt und nachhaltig gepflegt werden. Dafür SOLLTEN die relevanten Architekturelemente detailliert betrachtet werden, mindestens jedoch:

- zulässige Formen von Netzkomponenten inklusive virtualisierter Netzkomponenten,
- Festlegungen darüber, wie WAN- und Funkverbindungen abzusichern sind,
- Anbindung von Endgeräten an Switching-Komponenten, Verbindungen zwischen Netzelementen sowie Verwendung von Kommunikationsprotokollen,
- Redundanzmechanismen für alle Netzelemente,
- Adresskonzept für IPv4 und IPv6 sowie zugehörige Routing- und Switching-Konzepte,
- virtualisierte Netze in Virtualisierungs-Hosts inklusive NVO,

- Aufbau, Anbindung und Absicherung von Private Clouds sowie sichere Anbindung von Virtual Private Clouds, Hybrid Clouds und Public Clouds sowie
- Festlegungen zum Netzdesign für die sichere Administration und Überwachung der IT-Infrastruktur.

NET.1.1.A18 P-A-P-Struktur für die Internet-Anbindung (S)

Das Netz der Institution SOLLTE über eine Firewall mit P-A-P-Struktur an das Internet angeschlossen werden (siehe NET.1.1.A4 *Netztrennung in Zonen*).

Zwischen den beiden Firewall-Stufen MUSS ein proxy-basiertes Application-Layer-Gateway (ALG) realisiert werden. Das ALG MUSS über ein eigenes Transfernetz (dual-homed) sowohl zum äußeren Paketfilter als auch zum internen Paketfilter angebunden werden. Das Transfernetz DARF NICHT mit anderen Aufgaben als denjenigen für das ALG belegt sein.

Falls kein ALG eingesetzt wird, dann MÜSSEN entsprechende Sicherheits-Proxies realisiert werden. Die Sicherheits-Proxies MÜSSEN über ein eigenes Transfernetz (dual-homed) angebunden werden. Das Transfernetz DARF NICHT mit anderen Aufgaben als denjenigen für die Sicherheits-Proxies belegt sein. Es MUSS geprüft werden, ob über die Sicherheits-Proxies gegenseitige Angriffe möglich sind. Ist dies der Fall, MUSS das Transfernetz geeignet segmentiert werden.

Jeglicher Datenverkehr MUSS über das ALG oder entsprechende Sicherheits-Proxies entkoppelt werden. Ein Transfernetz, das beide Firewall-Stufen direkt miteinander verbindet, DARF NICHT konfiguriert werden. Die interne Firewall MUSS zudem die Angriffsfläche des ALGs oder der Sicherheits-Proxies gegenüber Innentätern und Innentäterinnen oder IT-Systemen im internen Netz reduzieren.

Authentisierte und vertrauenswürdige Netzzugriffe vom VPN-Gateway ins interne Netz SOLLTEN NICHT das ALG oder die Sicherheits-Proxies der P-A-P-Struktur durchlaufen.

NET.1.1.A19 Separierung der Infrastrukturdienste (S)

Server, die grundlegende Dienste für die IT-Infrastruktur bereitstellen, SOLLTEN in einem dedizierten Netzsegment positioniert werden. Die Kommunikation mit ihnen SOLLTE durch einen zustandsbehafteten Paketfilter (Firewall) kontrolliert werden.

NET.1.1.A20 Zuweisung dedizierter Subnetze für IPv4/IPv6-Endgerätegruppen (S)

Unterschiedliche IPv4-/IPv6- Endgeräte SOLLTEN je nach verwendetem Protokoll (IPv4-/IPv6- oder IPv4/IPv6-Dual-Stack) dedizierten Subnetzen zugeordnet werden.

NET.1.1.A21 Separierung des Management-Bereichs (S)

Um die Infrastruktur zu managen, SOLLTE durchgängig ein Out-of-Band-Management genutzt werden. Dabei SOLLTEN alle Endgeräte, die für das Management der IT-Infrastruktur benötigt werden, in dedizierten Netzsegmenten positioniert werden. Die Kommunikation mit diesen Endgeräten SOLLTE durch einen zustandsbehafteten Paketfilter kontrolliert werden. Die Kommunikation von und zu diesen Management-Netzsegmenten SOLLTE auf die notwendigen Management-Protokolle mit definierten Kommunikations-Endpunkten beschränkt werden.

Der Management-Bereich SOLLTE mindestens die folgenden Netzsegmente umfassen. Diese SOLLTEN abhängig von der Sicherheitsrichtlinie und der Anforderungsspezifikation weiter unterteilt werden in

- Netzsegment(e) für IT-Systeme, die für die Authentisierung und Autorisierung der administrativen Kommunikation zuständig sind,
- Netzsegment(e) für die Administration der IT-Systeme,
- Netzsegment(e) für die Überwachung und das Monitoring,
- Netzsegment(e), die die zentrale Protokollierung inklusive Syslog-Server und SIEM-Server enthalten,
- Netzsegment(e) für IT-Systeme, die für grundlegende Dienste des Management-Bereichs benötigt werden sowie
- Netzsegment(e) für die Management-Interfaces der zu administrierenden IT-Systeme.

Die verschiedenen Management-Interfaces der IT-Systeme MÜSSEN nach ihrem Einsatzzweck und ihrer Netzplatzierung über einen zustandsbehafteten Paketfilter getrennt werden. Dabei SOLLTEN die IT-Systeme (Management-Interfaces) zusätzlich bei folgender Zugehörigkeit über dedizierte Firewalls getrennt werden:

- IT-Systeme, die aus dem Internet erreichbar sind,
- IT-Systeme im internen Netz sowie
- Sicherheitskomponenten, die sich zwischen den aus dem Internet erreichbaren IT-Systemen und dem internen Netz befinden.

Es MUSS sichergestellt werden, dass die Segmentierung nicht durch die Management-Kommunikation unterlaufen werden kann. Eine Überbrückung von Netzsegmenten MUSS ausgeschlossen werden.

NET.1.1.A22 Spezifikation des Segmentierungskonzepts (S)

Auf Basis der Spezifikationen von Netzarchitektur und Netzdesign SOLLTE ein umfassendes Segmentierungskonzept für das interne Netz erstellt werden. Dieses Segmentierungskonzept SOLLTE eventuell vorhandene virtualisierte Netze in Virtualisierungs-Hosts beinhalten. Das Segmentierunskonzept SOLLTE geplant, umgesetzt, betrieben und nachhaltig gepflegt werden. Das Konzept SOLLTE mindestens die folgenden Punkte umfassen, soweit diese in der Zielumgebung vorgesehen sind:

- Initial anzulegende Netzsegmente und Vorgaben dazu, wie neue Netzsegmente zu schaffen sind und wie Endgeräte in den Netzsegmenten zu positionieren sind,
- Festlegung für die Segmentierung von Entwicklungs- und Testsystemen (Staging),
- Netzzugangskontrolle für Netzsegmente mit Clients,
- Anbindung von Netzbereichen, die über Funktechniken oder Standleitung an die Netzsegmente angebunden sind,
- Anbindung der Virtualisierungs-Hosts und von virtuellen Maschinen auf den Hosts an die Netzsegmente,
- Rechenzentrumsautomatisierung sowie
- Festlegungen dazu, wie Endgeräte einzubinden sind, die mehrere Netzsegmente versorgen, z. B. Load Balancer, und Speicher- sowie Datensicherungslösungen.

Abhängig von der Sicherheitsrichtlinie und der Anforderungsspezifikation SOLLTE für jedes Netzsegment konzipiert werden, wie es netztechnisch realisiert werden soll. Darüber hinaus SOLLTE festgelegt werden, welche Sicherheitsfunktionen die Koppelelemente zwischen den Netzsegmenten bereitstellen müssen (z. B. Firewall als zustandsbehafteter Paketfilter oder IDS/IPS).

NET.1.1.A23 Trennung von Netzsegmenten (S)

IT-Systeme mit unterschiedlichem Schutzbedarf SOLLTEN in verschiedenen Netzsegmenten platziert werden. Ist dies nicht möglich, SOLLTE sich der Schutzbedarf nach dem höchsten vorkommenden Schutzbedarf im Netzsegment richten. Darüber hinaus SOLLTEN die Netzsegmente abhängig von ihrer Größe und den Anforderungen des Segmentierungskonzepts weiter unterteilt werden. Es MUSS sichergestellt werden, dass keine Überbrückung von Netzsegmenten oder gar Zonen möglich ist.

Gehören die virtuellen LANs (VLANs) an einem Switch unterschiedlichen Institutionen an, SOLLTE die Trennung physisch erfolgen. Alternativ SOLLTEN Daten verschlüsselt werden, um die übertragenen Informationen vor unbefugtem Zugriff zu schützen.

NET.1.1.A24 Sichere logische Trennung mittels VLAN (S)

Falls VLANs eingesetzt werden, dann DARF dadurch KEINE Verbindung geschaffen werden zwischen dem internen Netz und einer Zone vor dem ALG oder den Sicherheits-Proxies.

Generell MUSS sichergestellt werden, dass VLANs nicht überwunden werden können.

NET.1.1.A25 Fein- und Umsetzungsplanung von Netzarchitektur und -design (S)

Eine Fein- und Umsetzungsplanung für die Netzarchitektur und das Netzdesign SOLLTE durchgeführt, dokumentiert, geprüft und nachhaltig gepflegt werden.

NET.1.1.A26 Spezifikation von Betriebsprozessen für das Netz (S)

Betriebsprozesse SOLLTEN bedarfsgerecht erzeugt oder angepasst und dokumentiert werden. Dabei SOLLTE insbesondere berücksichtigt werden, wie sich die Zonierung sowie das Segmentierungskonzept auf den IT-Betrieb auswirken.

NET.1.1.A27 Einbindung der Netzarchitektur in die Notfallplanung (S) [IT-Betrieb]

Es SOLLTE initial und in regelmäßigen Abständen nachvollziehbar analysiert werden, wie sich die Netzarchitektur und die abgeleiteten Konzepte auf die Notfallplanung auswirken.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.1.1.A28 Hochverfügbare Netz- und Sicherheitskomponenten (H)

Zentrale Bereiche des internen Netzes sowie die Sicherheitskomponenten SOLLTEN hochverfügbar ausgelegt sein. Dazu SOLLTEN die Komponenten redundant ausgelegt und auch intern hochverfügbar realisiert werden.

NET.1.1.A29 Hochverfügbare Realisierung von Netzanbindungen (H)

Die Netzanbindungen, wie z. B. Internet-Anbindung und WAN-Verbindungen, SOLLTEN vollständig redundant gestaltet werden. Je nach Verfügbarkeitsanforderung SOLLTEN redundante Anbindungen an Dienstleistende bedarfsabhängig mit unterschiedlicher Technik und Performance bedarfsgerecht umgesetzt werden. Auch SOLLTE Wegeredundanz innerhalb und außerhalb der eigenen Zuständigkeit bedarfsgerecht umgesetzt werden. Dabei SOLLTEN mögliche Single Points of Failures (SPoF) und störende Umgebungsbedingungen berücksichtigt werden.

NET.1.1.A30 Schutz vor Distributed-Denial-of-Service (H)

Um DDoS-Angriffe abzuwehren, SOLLTE per Bandbreitenmanagement die verfügbare Bandbreite gezielt zwischen verschiedenen Kommunikationspartnern und -partnerinnen sowie Protokollen aufgeteilt werden.

Um DDoS-Angriffe mit sehr hohen Datenraten abwehren zu können, SOLLTEN Mitigation-Dienste über größere Internet Service Provider (ISPs) eingekauft werden. Deren Nutzung SOLLTE in Verträgen geregelt werden.

NET.1.1.A31 Physische Trennung von Netzsegmenten (H)

Abhängig von Sicherheitsrichtlinie und Anforderungsspezifikation SOLLTEN Netzsegmente physisch durch separate Switches getrennt werden.

NET.1.1.A32 Physische Trennung von Management-Netzsegmenten (H)

Abhängig von Sicherheitsrichtlinie und Anforderungsspezifikation SOLLTEN Netzsegmente des Management-Bereichs physisch voneinander getrennt werden.

NET.1.1.A33 Mikrosegmentierung des Netzes (H)

Das Netz SOLLTE in kleine Netzsegmente mit sehr ähnlichem Anforderungsprofil und selbem Schutzbedarf unterteilt werden. Insbesondere SOLLTE dies für die DMZ-Segmente berücksichtigt werden.

NET.1.1.A34 Einsatz kryptografischer Verfahren auf Netzebene (H)

Die Netzsegmente SOLLTEN im internen Netz, im Extranet und im DMZ-Bereich mittels kryptografischer Techniken bereits auf Netzebene realisiert werden. Dafür SOLLTEN VPN-Techniken oder IEEE 802.1AE eingesetzt werden.

Wenn innerhalb von internem Netz, Extranet oder DMZ über Verbindungsstrecken kommuniziert wird, die für einen erhöhten Schutzbedarf nicht ausreichend sicher sind, SOLLTE die Kommunikation angemessen auf Netzebene verschlüsselt werden.

NET.1.1.A35 Einsatz von netzbasiertem DLP (H)

Auf Netzebene SOLLTEN Systeme zur Data Lost Prevention (DLP) eingesetzt werden.

NET.1.1.A36 Trennung mittels VLAN bei sehr hohem Schutzbedarf (H)

Bei sehr hohem Schutzbedarf SOLLTEN KEINE VLANs eingesetzt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld Netze veröffentlicht:

- Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)
- Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf: BSI-TL-02103 – Version 2.0

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27033 „Information technology – Security techniques – Network security – Part 1: Overview and concepts bis Part 3: Reference networking scenarios – Threats, design techniques and control issues“ Vorgaben für die Absicherung von Netzen.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.1.2 Netzmanagement

1. Beschreibung

1.1. Einleitung

Ein zuverlässiges Netzmanagement ist Grundvoraussetzung für den sicheren und effizienten Betrieb moderner Netze. Dazu ist es erforderlich, dass das Netzmanagement alle Netzkomponenten umfassend integriert. Außerdem müssen geeignete Maßnahmen umgesetzt werden, um die Netzmanagement-Kommunikation und -infrastruktur zu schützen.

Das Netzmanagement umfasst viele wichtige Funktionen wie z. B. die Netzüberwachung, die Konfiguration der Komponenten, die Behandlung von Ereignissen und die Protokollierung. Eine weitere wichtige Funktion ist das Reporting, das als gemeinsame Plattform für Netz und IT-Systeme angelegt werden kann. Alternativ kann es dediziert als einheitliche Plattform oder als Bestandteil der einzelnen Netzmanagement-Komponenten realisiert werden.

Die Netzmanagement-Infrastruktur besteht aus zentralen Management-Systemen, wie z. B. einem SNMP-Server, Administrations-Endgeräten mit Software für Managementzugriffe und dezentralen Managementagenten. Außerdem gehören dedizierte Managementwerkzeuge, wie z. B. Probes bzw. spezifische Messgeräte sowie Managementprotokolle, wie z. B. SNMP oder SSH, dazu. Auch Managementschnittstellen, wie dedizierte Ethernet-Ports oder Konsolen-Ports, sind Bestandteil einer Netzmanagement-Infrastruktur.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil des Netzmanagements zu etablieren.

1.3. Abgrenzung und Modellierung

Der Baustein NET.1.2 *Netzmanagement* ist auf jedes Netzmanagement-System (Management-System und zu verwaltende IT-System) anzuwenden, das im Informationsverbund eingesetzt wird. Bei den zu verwaltenden IT-Systemen handelt es sich üblicherweise um einzelne Clients, Server oder aktive Netzkomponenten (Netzkoppelelemente).

Dieser Baustein betrachtet die notwendigen Komponenten und konzeptionellen Aufgaben zum Netzmanagement. Anforderungen zum Systemmanagement für vernetzte Clients und Server werden hier nicht beschrieben.

Der vorliegende Baustein beschreibt, wie das Netzmanagement aufgebaut und abgesichert sowie die zugehörige Kommunikation geschützt werden können. Details bezüglich der Absicherung von Netzkomponenten, insbesondere deren Management-Schnittstellen, werden in den Bausteinen der Schichten NET.2 *Funknetze* und NET.3 *Netzkomponenten* behandelt.

Die in diesem Baustein thematisierte Protokollierung sollte in ein übergreifendes Protokollierungs- und Archivierungskonzept eingebunden sein (siehe OPS.1.1.5 *Protokollierung* und OPS.1.2.2 *Archivierung*).

Die Daten des Netzmanagements müssen im Datensicherungskonzept berücksichtigt werden. Anforderungen dazu sind im Baustein CON.3 *Datensicherungskonzept* enthalten.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.1.2 *Netzmanagement* von besonderer Bedeutung.

2.1. Unberechtigter Zugriff auf zentrale Netzmanagement-Komponenten

Wenn es bei einem Angriff gelingt, auf Netzmanagement-Lösungen zuzugreifen, z. B. durch ungepatchte Sicherheitslücken oder eine ungenügende Netztrennung, können alle dort angeschlossenen Netzkomponenten kontrolliert und neu konfiguriert werden. So kann z. B. auf schützenswerte Informationen zugegriffen, der Netzverkehr umgeleitet oder auch das gesamte Netz nachhaltig gestört werden.

2.2. Unberechtigter Zugriff auf einzelne Netzkomponenten

Wenn es bei einem Angriff gelingt, auf einzelne Netzkomponenten zuzugreifen, kann die jeweilige Komponente kontrolliert und manipuliert werden. Jeder über die Netzkomponente geleitete Datenverkehr kann somit kompromittiert werden. Darüber hinaus können weiterführende Angriffe vorbereitet werden, um tiefer in das Netz der Institution einzudringen.

2.3. Unberechtigte Eingriffe in die Netzmanagement-Kommunikation

Wird die Netzmanagement-Kommunikation abgehört und manipuliert, können auf diesem Weg aktive Netzkomponenten fehlkonfiguriert bzw. kontrolliert werden. Dadurch kann die Netzintegrität verletzt und die Verfügbarkeit der Netzinfrastruktur eingeschränkt werden. Außerdem können die übertragenen Daten mitgeschnitten und eingesehen werden.

2.4. Unzureichende Zeitsynchronisation der Netzmanagement-Komponenten

Wird die Systemzeit der Netzmanagement-Komponenten unzureichend synchronisiert, können die Protokollierungsdaten eventuell nicht miteinander korreliert werden. Auch kann die Korrelation eventuell zu fehlerhaften Aussagen führen, da die unterschiedlichen Zeitstempel von Ereignissen keine gemeinsame Basis aufweisen. So kann nicht geeignet auf Ereignisse reagiert werden. Probleme können zudem nicht beseitigt werden. Dadurch können beispielsweise Sicherheitsvorfälle und Datenabflüsse unerkannt bleiben.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.1.2 *Netzmanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Planende, Vorgesetzte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.1.2.A1 Planung des Netzmanagements (B)

Die Netzmanagement-Infrastruktur MUSS geeignet geplant werden. Dabei SOLLTEN alle in der Sicherheitsrichtlinie und Anforderungsspezifikation für das Netzmanagement genannten Punkte berücksichtigt werden. Es MÜSSEN mindestens folgende Themen berücksichtigt werden:

- zu trennende Bereiche für das Netzmanagement,
- Zugriffsmöglichkeiten auf die Management-Server,
- Kommunikation für den Managementzugriff,
- eingesetzte Protokolle, z. B. IPv4 und IPv6,
- Anforderungen an Management-Werkzeuge,
- Schnittstellen, um erfasste Ereignis- oder Alarmmeldungen weiterzuleiten,
- Protokollierung, inklusive erforderlicher Schnittstellen zu einer zentralen Protokollierungslösung,
- Reporting und Schnittstellen zu übergreifenden Lösungen sowie
- korrespondierende Anforderungen an die einzubindenden Netzkomponenten.

NET.1.2.A2 Anforderungsspezifikation für das Netzmanagement (B)

Ausgehend von NET.1.2.A1 *Planung des Netzmanagements* MÜSSEN Anforderungen an die Netzmanagement-Infrastruktur und -Prozesse spezifiziert werden. Dabei MÜSSEN alle wesentlichen Elemente für das Netzmanagement berücksichtigt werden. Auch SOLLTE die Richtlinie für das Netzmanagement beachtet werden.

NET.1.2.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.1.2.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.1.2.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.1.2.A6 Regelmäßige Datensicherung (B)

Bei der Datensicherung des Netzmanagements MÜSSEN mindestens die Systemdaten für die Einbindung der zu verwaltenden Komponenten bzw. Objekte, Ereignismeldungen, Statistikdaten sowie vorgehaltene Daten für das Konfigurationsmanagement gesichert werden.

NET.1.2.A7 Grundlegende Protokollierung von Ereignissen (B)

Mindestens folgende Ereignisse MÜSSEN protokolliert werden:

- unerlaubte Zugriffe bzw. Zugriffsversuche,
- Leistungs- oder Verfügbarkeitsschwankungen des Netzes,
- Fehler in automatischen Prozessen (z. B. bei der Konfigurationsverteilung) sowie
- eingeschränkte Erreichbarkeit von Netzkomponenten.

NET.1.2.A8 Zeit-Synchronisation (B)

Alle Komponenten des Netzmanagements, inklusive der eingebundenen Netzkomponenten, MÜSSEN eine synchrone Uhrzeit nutzen. Die Uhrzeit SOLLTE an jedem Standort innerhalb des lokalen Netzes mittels NTP-Service synchronisiert werden. Ist ein separates Managementnetz eingerichtet, SOLLTE eine NTP-Instanz in diesem Managementnetz positioniert werden.

NET.1.2.A9 Absicherung der Netzmanagement-Kommunikation und des Zugriffs auf Netz-Management-Werkzeuge (B)

Erfolgt die Netzmanagement-Kommunikation über die produktive Infrastruktur, MÜSSEN dafür sichere Protokolle verwendet werden. Ist dies nicht möglich, MUSS ein eigens dafür vorgesehenes Administrationsnetz (Out-of-Band-Management) verwendet werden (siehe NET.1.1 *Netzarchitektur und -design*).

Falls von einem Netz außerhalb der Managementnetze auf Netzmanagement-Werkzeuge zugegriffen wird, MÜSSEN als sicher geltende Authentisierungs- und Verschlüsselungsmethoden realisiert werden.

NET.1.2.A10 Beschränkung der SNMP-Kommunikation (B)

Grundsätzlich DÜRFEN im Netzmanagement KEINE unsicheren Versionen des Simple Network Management Protocol (SNMP) eingesetzt werden. Werden dennoch unsichere Protokolle verwendet und nicht über andere sichere Netzprotokolle (z. B. VPN oder TLS) abgesichert, MUSS ein separates Managementnetz genutzt werden. Grundsätzlich SOLLTE über SNMP nur mit den minimal erforderlichen Zugriffsrechten zugegriffen werden. Die Zugangsberechtigung SOLLTE auf dedizierte Management-Server eingeschränkt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.1.2.A11 Festlegung einer Sicherheitsrichtlinie für das Netzmanagement (S)

Für das Netzmanagement SOLLTE eine Sicherheitsrichtlinie erstellt und nachhaltig gepflegt werden. Die Sicherheitsrichtlinie SOLLTE allen Personen, die am Netzmanagement beteiligt sind, bekannt sein. Die Sicherheitsrichtlinie SOLLTE zudem grundlegend für ihre Arbeit sein. Es SOLLTE regelmäßig und nachvollziehbar überprüft werden, dass die in der Sicherheitsrichtlinie geforderten Inhalte umgesetzt werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

Die Sicherheitsrichtlinie SOLLTE festlegen, welche Bereiche des Netzmanagements über zentrale Management-Werkzeuge und -Dienste realisiert werden. Auch SOLLTE sie definieren, inwieweit Aufgaben im Netzmanagement der Institution automatisiert realisiert werden sollen.

Darüber hinaus SOLLTEN Rahmenbedingungen und Vorgaben für die Netztrennung, die Zugriffskontrolle, die Protokollierung sowie für den Schutz der Kommunikation spezifiziert werden. Auch für das eingesetzte Netzmanagement-Werkzeug und für die operativen Grundregeln des Netzmanagements SOLLTEN Rahmenbedingungen und Vorgaben spezifiziert werden.

NET.1.2.A12 Ist-Aufnahme und Dokumentation des Netzmanagements (S)

Es SOLLTE eine Dokumentation erstellt werden, die beschreibt, wie die Management-Infrastruktur des Netzes aufgebaut ist. Darin SOLLTEN die initiale Ist-Aufnahme sowie alle durchgeführten Änderungen im Netzmanagement enthalten sein. Insbesondere SOLLTE dokumentiert werden, welche Netzkomponenten mit welchen Management-Werkzeugen verwaltet werden. Außerdem SOLLTEN alle für das Netzmanagement benutzten IT-Arbeitsplätze und -Endgeräte sowie alle Informationsbestände, Management-Daten und Informationen über den Betrieb des Netzmanagements erfasst werden. Letztlich SOLLTEN sämtliche Schnittstellen zu Anwendungen und Diensten außerhalb des Netzmanagements dokumentiert werden.

Der so dokumentierte Ist-Zustand der Management-Infrastruktur SOLLTE mit der Dokumentation der Netz-Infrastruktur abgeglichen werden (siehe Baustein NET.1.1 *Netz-Architektur- und Design).*

Die Dokumentation SOLLTE vollständig und immer aktuell sein.

NET.1.2.A13 Erstellung eines Netzmanagement-Konzepts (S)

Ausgehend von der Sicherheitsrichtlinie für das Netzmanagement SOLLTE ein Netzmanagement-Konzept erstellt und nachhaltig gepflegt werden. Dabei SOLLTEN mindestens folgende Aspekte bedarfsgerecht berücksichtigt werden:

- Methoden, Techniken und Werkzeuge für das Netzmanagement,
- Absicherung des Zugangs und der Kommunikation,

- Netztrennung, insbesondere Zuordnung von Netzmanagement-Komponenten zu Zonen,
- Umfang des Monitorings und der Alarmierung je Netzkomponente,
- Protokollierung,
- Automatisierung, insbesondere zentrale Verteilung von Konfigurationsdateien auf Switches,
- Meldeketten bei Störungen und Sicherheitsvorfällen,
- Bereitstellung von Netzmanagement-Informationen für andere Betriebsbereiche sowie
- Einbindung des Netzmanagements in die Notfallplanung.

NET.1.2.A14 Fein- und Umsetzungsplanung (S)

Es SOLLTE eine Fein- und Umsetzungsplanung für die Netzmanagement-Infrastruktur erstellt werden. Dabei SOLLTEN alle in der Sicherheitsrichtlinie und im Netzmanagement-Konzept adressierten Punkte berücksichtigt werden.

NET.1.2.A15 Konzept für den sicheren Betrieb der Netzmanagement-Infrastruktur (S)

Ausgehend von der Sicherheitsrichtlinie für das Netzmanagement und dem Netzmanagement-Konzept SOLLTE ein Konzept für den sicheren Betrieb der Netzmanagement-Infrastruktur erstellt werden. Darin SOLLTE der Anwendungs- und Systembetrieb für die Netzmanagement-Werkzeuge berücksichtigt werden. Auch SOLLTE geprüft werden, wie sich die Leistungen anderer operativer Einheiten einbinden und steuern lassen.

NET.1.2.A16 Einrichtung und Konfiguration von Netzmanagement-Lösungen (S)

Lösungen für das Netzmanagement SOLLTEN anhand der Sicherheitsrichtlinie, der spezifizierten Anforderungen (siehe NET1.2.A2 *Anforderungsspezifikation für das Netzmanagement*) und der Fein- und Umsetzungsplanung aufgebaut, sicher konfiguriert und in Betrieb genommen werden. Danach SOLLTEN die spezifischen Prozesse für das Netzmanagement eingerichtet werden.

NET.1.2.A17 Regelmäßiger Soll-Ist-Vergleich im Rahmen des Netzmanagements (S)

Es SOLLTE regelmäßig und nachvollziehbar geprüft werden, inwieweit die Netzmanagement-Lösung dem Sollzustand entspricht. Dabei SOLLTE geprüft werden, ob die bestehende Lösung noch die Sicherheitsrichtlinie und Anforderungsspezifikation erfüllt. Auch SOLLTE geprüft werden, inwieweit die umgesetzte Management-Struktur und die genutzten Prozesse dem aktuellen Stand entsprechen. Weiter SOLLTE verglichen werden, ob die Management-Infrastruktur aktuell ist.

NET.1.2.A18 Schulungen für Management-Lösungen (S) [Vorgesetzte]

Für die eingesetzten Netzmanagement-Lösungen SOLLTEN Schulungs- und Trainingsmaßnahmen konzipiert und durchgeführt werden. Die Maßnahmen SOLLTEN die individuellen Gegebenheiten im Configuration-, Availability- und Capacity-Management sowie typische Situationen im Fehlermanagement abdecken. Die Schulungen und Trainings SOLLTEN regelmäßig wiederholt werden, mindestens jedoch, wenn sich größere technische oder organisatorische Änderungen innerhalb der Netzmanagement-Lösung ergeben.

NET.1.2.A19 ENTFALLEN (S)

Diese Anforderung ist entfallen.

NET.1.2.A20 ENTFALLEN (S)

Diese Anforderung ist entfallen.

NET.1.2.A21 Entkopplung der Netzmanagement-Kommunikation (S)

Direkte Management-Zugriffe von Administrierenden von einem IT-System außerhalb der Managementnetze auf eine Netzkomponente SOLLTEN vermieden werden. Ist ein solcher Zugriff ohne zentrales Management-Werkzeug notwendig, SOLLTE die Kommunikation entkoppelt werden. Solche Sprungserver SOLLTEN im Management-Netz integriert und in einem getrennten Zugangssegment positioniert sein.

NET.1.2.A22 Beschränkung der Management-Funktionen (S)

Es SOLLTEN nur die benötigten Management-Funktionen aktiviert werden.

NET.1.2.A23 ENTFALLEN (S)

Diese Anforderung ist entfallen.

NET.1.2.A24 Zentrale Konfigurationsverwaltung für Netzkomponenten (S)

Software bzw. Firmware und Konfigurationsdaten für Netzkomponenten SOLLTEN automatisch über das Netz verteilt und ohne Betriebsunterbrechung installiert und aktiviert werden können. Die dafür benötigten Informationen SOLLTEN an zentraler Stelle sicher verfügbar sein sowie in die Versionsverwaltung und die Datensicherung eingebunden werden. Die zentrale Konfigurationsverwaltung SOLLTE nachhaltig gepflegt und regelmäßig auditiert werden.

NET.1.2.A25 Statusüberwachung der Netzkomponenten (S)

Die grundlegenden Performance- und Verfügbarkeitsparameter der zentralen Netzkomponenten SOLLTEN kontinuierlich überwacht werden. Dafür SOLLTEN vorab die jeweiligen Schwellwerte ermittelt werden (Baselining).

NET.1.2.A26 Alarming und Logging (S)

Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-Werkzeugen SOLLTEN automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden (siehe OPS.1.1.5 *Protokollierung*). Das zuständige Personal SOLLTE zusätzlich automatisch benachrichtigt werden. Das Alarming und Logging SOLLTE mindestens folgende Punkte beinhalten:

- Ausfall bzw. Nichterreichbarkeit von Netz- oder Management-Komponenten,
- Hardware-Fehlfunktionen,
- fehlerhafte Anmeldeversuche sowie
- kritische Zustände oder Überlastung von IT-Systemen.

Ereignismeldungen bzw. Logging-Daten SOLLTEN einem zentralen Management-System entweder kontinuierlich oder gebündelt übermittelt werden. Alarmmeldungen SOLLTEN sofort wenn sie auftreten übermittelt werden.

NET.1.2.A27 Einbindung des Netzmanagements in die Notfallplanung (S)

Die Netzmanagement-Lösungen SOLLTEN in die Notfallplanung der Institution eingebunden werden. Dazu SOLLTEN die Netzmanagement-Werkzeuge und die Konfigurationen der Netzkomponenten gesichert und in die Wiederanlaufpläne integriert sein.

NET.1.2.A28 Platzierung der Management-Clients für das In-Band-Management (S)

Für die Administration sowohl der internen als auch der externen IT-Systeme SOLLTEN dedizierte Management-Clients eingesetzt werden. Dafür SOLLTE mindestens ein Management-Client am äußeren Netzbereich (für die Administration am Internet anliegender IT-Systeme) und ein weiterer im internen Bereich (für die Administration interner IT-Systeme) platziert werden.

NET.1.2.A29 Einsatz von VLANs im Management-Netz (S)

Werden Managementnetze durch VLANs getrennt, SOLLTE darauf geachtet werden, dass der äußere Paketfilter sowie die daran angeschlossenen Geräte in einem eigenen Teilnetz stehen. Zudem SOLLTE sichergestellt werden, dass das ALG dabei nicht umgangen wird.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.1.2.A30 Hochverfügbare Realisierung der Management-Lösung (H)

Zentrale Management-Lösungen SOLLTEN hochverfügbar betrieben werden. Dazu SOLLTEN die Server bzw. Werkzeuge inklusive der Netzanbindungen redundant ausgelegt sein. Auch die einzelnen Komponenten SOLLTEN hochverfügbar bereitgestellt werden.

NET.1.2.A31 Grundsätzliche Nutzung von sicheren Protokollen (H)

Für das Netzmanagement SOLLTEN ausschließlich sichere Protokolle benutzt werden. Es SOLLTEN alle Sicherheitsfunktionen dieser Protokolle verwendet werden.

NET.1.2.A32 Physische Trennung des Managementnetzes (H) [Planende]

Das Managementnetz SOLLTE physisch von den produktiven Netzen getrennt werden.

NET.1.2.A33 Physische Trennung von Management-Segmenten (H) [Planende]

Es SOLLTEN physisch getrennte Zonen mindestens für das Management von LAN-Komponenten, Sicherheitskomponenten und Komponenten zur Außenanbindung eingerichtet werden.

NET.1.2.A34 ENTFALLEN (H)

Diese Anforderung ist entfallen.

NET.1.2.A35 Festlegungen zur Beweissicherung (H)

Die erhobenen Protokollierungsdaten SOLLTEN für forensische Analysen gesetzeskonform und revisionssicher archiviert werden (siehe auch DER.2.2 *Vorsorge für die IT-Forensik*).

NET.1.2.A36 Einbindung der Protokollierung des Netzmanagements in eine SIEM-Lösung (H)

Die Protokollierung des Netzmanagements SOLLTE in eine Security-Information-and-Event-Management (SIEM)-Lösung eingebunden werden. Dazu SOLLTEN die Anforderungskataloge zur Auswahl von Netzmanagement-Lösungen hinsichtlich der erforderlichen Unterstützung von Schnittstellen und Übergabeformaten angepasst werden (siehe NET.1.2.A2 *Anforderungsspezifikation für das Netzmanagement*).

NET.1.2.A37 Standortübergreifende Zeitsynchronisation (H)

Die Zeitsynchronisation SOLLTE über alle Standorte der Institution sichergestellt werden. Dafür SOLLTE eine gemeinsame Referenzzeit benutzt werden.

NET.1.2.A38 Festlegung von Notbetriebsformen für die Netzmanagement-Infrastruktur (H)

Für eine schnelle Wiederherstellung der Sollzustände von Software bzw. Firmware sowie der Konfiguration der Komponenten in der Netzmanagement-Infrastruktur SOLLTEN hinreichend gute Ersatzlösungen festgelegt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) formuliert in der Norm ISO/IEC 27033 „Information technology – Security techniques – Network security – Part 1: Overview and concepts bis Part 3: Reference networking scenarios – Threats, design techniques and control issues" Vorgaben für die Absicherung von Netzen.

Das BSI hat das weiterführende Dokument „Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)" zum Themenfeld Netzmanagement veröffentlicht.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.2.1 WLAN-Betrieb

1. Beschreibung

1.1. Einleitung

Über Wireless LANs (WLANs) können drahtlose lokale Netze aufgebaut oder bestehende drahtgebundene Netze erweitert werden. Bis heute basieren fast alle am Markt verfügbaren WLAN-Komponenten auf dem Standard IEEE 802.11 und seinen Ergänzungen. Eine besondere Rolle nimmt dabei das Firmenkonsortium „Wi-Fi Alliance" ein, das basierend auf dem Standard IEEE 802.11 mit „Wi-Fi" einen Industriestandard geschaffen hat. Dabei bestätigt die Wi-Fi Alliance mit dem Wi-Fi-Gütesiegel, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat.

Innerhalb von Institutionen können WLANs eingesetzt werden, um flexibel mit mobilen Geräten zu arbeiten und diesen den Zugang zum Netz der Institution zu ermöglichen. Hierfür werden innerhalb der Institution Netzzugänge über so genannten Access Points aufgebaut. Aufgrund der meist einfachen und schnellen Installation werden WLANs auch dazu eingesetzt, um temporär Netze einzurichten, beispielsweise auf Messen oder kleineren Veranstaltungen. Darüber hinaus können an öffentlichen Plätzen, wie Flughäfen oder Bahnhöfen, Netzzugänge über so genannte Hotspots angeboten werden. Dadurch werden den mobilen Benutzenden Verbindungen in das Internet oder ihr Institutionsnetz ermöglicht. Die Kommunikation findet dann generell zwischen einem zentralen Zugangspunkt, dem Access Point, und der WLAN-Komponente des Endgeräts statt.

1.2. Zielsetzung

In diesem Baustein wird systematisch aufgezeigt, wie WLANs sicher in einer Institution aufgebaut und betrieben werden können.

1.3. Abgrenzung und Modellierung

Der Baustein NET.2.1 *WLAN-Betrieb* ist auf alle Kommunikationsnetze anzuwenden, die gemäß der Standard-Reihe IEEE 802.11 und deren Erweiterungen aufgebaut und betrieben werden.

Der Baustein enthält grundsätzliche Anforderungen, die beachtet und erfüllt werden müssen, wenn WLANs in Institutionen aufgebaut und betrieben werden. Anforderungen für eine sichere Nutzung von WLANs sind jedoch nicht Gegenstand dieses Bausteins. Die sichere Nutzung von WLANs wird im Baustein NET.2.2 *WLAN-Nutzung* behandelt.

WLANs können entsprechend den Bedürfnissen der betreibenden Institution und der Hardware-Ausstattung, die zur Verfügung steht, in zwei verschiedenen Modi betrieben werden. Im Ad-hoc-Modus kommunizieren zwei oder mehr WLAN-Clients direkt miteinander. WLANs im Ad-hoc-Modus können sich selbstständig, also ohne feste Infrastruktur, aufbauen und konfigurieren. Somit können sie eine vollvermaschte parallele Netz-Infrastruktur etablieren. Dadurch ist der Ad-hoc-Modus in einer zu schützenden Umgebung ungeeignet und wird deshalb im Folgenden nicht weiter betrachtet. In den meisten Fällen werden WLANs im Infrastruktur-Modus betrieben, d. h. die Kommunikation der WLAN-Clients und die Verbindung in kabelgebundene LAN-Segmente erfolgt über Access Points.

Werden für die Authentisierung am WLAN entsprechende Dienste (z. B. RADIUS) eingesetzt, so müssen die entsprechenden IT-Systeme, auf denen die Dienste betrieben werden, gesondert abgesichert werden. Hierfür können die Bausteine der Schicht SYS.1, wie zum Beispiel SYS.1.1 *Allgemeiner Server,* herangezogen werden.

Wird ein WLAN betrieben, sollte dieses grundsätzlich mit berücksichtigt werden, wenn die Bausteine NET.1.1 *Netzarchitektur und -design*, NET.1.2 *Netzmanagement* und DER.2.1 *Behandlung von Sicherheitsvorfällen* umgesetzt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.2.1 *WLAN-Betrieb* von besonderer Bedeutung.

2.1. Ausfall oder Störung eines Funknetzes

In Funknetzen werden Informationen mittels elektromagnetischer Funkwellen übertragen. Strahlen andere elektromagnetische Quellen im selben Frequenzspektrum Energie ab, können diese die drahtlose Kommunikation stören und im Extremfall den Betrieb des WLANs verhindern. Dies kann durch andere Funksysteme und Geräte, wie beispielsweise Bluetooth, Mikrowellenherde oder andere WLAN-Netze hervorgerufen werden. Darüber hinaus sind auch Denial-of-Service-Angriffe möglich. Werden beispielsweise bestimmte Steuer- und Managementsignale wiederholt gesendet, kann dies dazu führen, dass das Funknetz nicht mehr verfügbar ist.

2.2. Fehlende oder unzureichende Planung des WLAN-Einsatzes

Fehler in der Planung stellen sich oft als besonders schwerwiegend heraus, weil dadurch leicht flächendeckende Sicherheitslücken geschaffen werden können. Wird der Einsatz von WLANs nicht oder nur unzureichend geplant, kann sich eine Vielzahl von Problemen ergeben, beispielsweise:

- Vertrauliche Daten könnten mitgelesen werden, etwa wenn WLAN-Standards eingesetzt werden, die nicht mehr dem Stand der Technik entsprechen (z. B. WEP zur Verschlüsselung).
- Die Übertragungskapazität könnte unzureichend sein. Dadurch können bandbreitenintensive Anwendungen nicht mit der erforderlichen Dienstgüte genutzt werden.
- Die Abdeckung des WLANs könnte nicht ausreichend sein, sodass an bestimmten Orten kein Netz verfügbar ist.

2.3. Fehlende oder unzureichende Regelungen zum WLAN-Einsatz

Bei einer WLAN-Infrastruktur, die nicht zentral administriert wird, sind die Access Points in der Standard-Einstellung meist ohne oder nur mit unzureichenden Sicherheitsmechanismen vorkonfiguriert. Schließen Mitarbeitende beispielsweise aufgrund fehlender Regelungen einen ungenehmigten bzw. ungesicherten Access Point an ein internes Netz der Institution an, kann dies zu schwerwiegenden Problemen führen. Denn sie untergraben damit praktisch sämtliche innerhalb des LANs ergriffenen Sicherheitsmaßnahmen, wie z. B. die Firewall zum Schutz gegen unberechtigte externe Zugriffe.

2.4. Ungeeignete Auswahl von Authentisierungsverfahren

Wenn Authentisierungsverfahren und -mechanismen fehlen oder unzureichend sind, können Sicherheitslücken entstehen. Beispielsweise wird im Standard IEEE 802.1X (Port Based Network Access Control) das Extensible Authentication Protocol (EAP) definiert. In einigen der beschriebenen EAP-Methoden sind aber Schwachstellen enthalten. So ist EAP-MD5 etwa anfällig gegenüber Man-in-the-Middle- und Wörterbuchangriffen. Wird EAP-MD5 eingesetzt, können Passwörter erraten werden. Außerdem kann die Kommunikation abgehört werden.

2.5. Fehlerhafte Konfiguration der WLAN-Infrastruktur

Access Points und andere WLAN-Komponenten (z. B. WLAN Controller) bieten eine Vielzahl von Konfigurationseinstellungen, die insbesondere auch Sicherheitsfunktionen betreffen. Werden diese falsch konfiguriert, ist entweder keine Kommunikation über einen Access Point möglich oder die Kommunikation erfolgt ungeschützt bzw. mit einem zu geringen Schutzniveau.

2.6. Unzureichende oder fehlende WLAN-Sicherheitsmechanismen

Im Auslieferungszustand sind WLAN-Komponenten häufig so konfiguriert, dass keine oder nur wenige Sicherheitsmechanismen aktiviert sind. Einige der Mechanismen sind darüber hinaus unzureichend und bieten somit keinen ausreichenden Schutz. Auch heute werden noch diverse WLAN-Komponenten eingesetzt, die lediglich unzureichende Sicherheitsmechanismen wie z. B. WEP unterstützen. Teilweise können diese Geräte nicht einmal auf stärkere Sicherheitsmechanismen aufgerüstet werden. Werden solche Geräte eingesetzt, können Angreifende leicht die gesamte Kommunikation abhören und damit vertrauliche Informationen einsehen.

2.7. Abhören der WLAN-Kommunikation

Da es sich bei Funk um ein Medium handelt, das sich mehrere Benutzende teilen können („Shared Medium"), können die über WLANs übertragenen Daten problemlos mitgehört und aufgezeichnet werden. Wenn die Daten nicht oder nur unzureichend verschlüsselt werden, können die übertragenen Nutzdaten leicht eingesehen werden. Zudem überschreiten Funknetze bzw. die ausgesendeten Funkwellen häufig die Grenzen der selbst genutzten Räumlichkeiten. So werden Daten auch noch in Bereiche ausgestrahlt, die nicht von den Benutzenden oder einer Institution kontrolliert und gesichert werden können.

2.8. Vortäuschung eines gültigen Access Points (Rogue Access Point)

Angreifende können sich als Teil der WLAN-Infrastruktur ausgeben, indem sie einen eigenen Access Point mit einem geeignet gewählten Namen (SSID) in der Nähe eines WLAN-Clients installiert. Dieser vorgetäuschte Access Point wird als „Rogue Access Point" bezeichnet. Bietet dieser dem WLAN-Client eine stärkere Sendeleistung als der echte Access Point, wird der Client diesen als Basisstation nutzen, falls diese sich nicht gegenseitig authentisieren. Zusätzlich könnte auch der echte Access Point durch einen Denial-of-Service-Angriff ausgeschaltet werden. Die Benutzenden melden sich an einem Netz an, das nur vorgibt, das Zielnetz zu sein. Dadurch ist es Angreifenden möglich, die Kommunikation abzuhören. Auch durch Poisoning- oder Spoofing-Methoden können Angreifende eine falsche Identität vortäuschen bzw. den Netzverkehr zu ihren IT-Systemen umlenken. So können sie die Kommunikation belauschen und kontrollieren. Besonders in öffentlichen Funknetzen (sogenannten Hotspots) ist ein Rogue Access Point ein beliebtes Angriffsmittel.

2.9. Ungeschützter LAN-Zugang am Access Point

Sind Access Points sichtbar und ohne physischen Schutz montiert, können sich Angreifende zwischen die Access Points und die Switch-Infrastruktur schalten, um den gesamten Netzverkehr abzuhören. Selbst wenn die drahtlose Kommunikation mit WPA2 verschlüsselt wird, stellt dies eine Gefährdung dar, weil diese Methoden nur die Luftschnittstelle absichern, die Ethernet-Anbindung aber nicht weiter berücksichtigen.

2.10. Hardware-Schäden

Hardware-Schäden können dazu führen, dass der Funkverkehr gestört wird. Im schlimmsten Fall kann das WLAN sogar komplett ausfallen. Dies betrifft insbesondere WLAN-Geräte, die außerhalb von geschützten Räumen angebracht werden, z. B. um offene Plätze abzudecken. Sie sind zusätzlichen Gefährdungen ausgesetzt, wie beispielsweise vorsätzlichen Beschädigungen durch Angreifende oder umweltbedingten Schäden durch Witterung oder Blitzeinschlag.

2.11. Diebstahl eines Access Points

Werden WLAN Access Points ungesichert in öffentlichen Bereichen installiert, können sie gestohlen werden. Dadurch lässt sich beispielsweise ein Shared-Secret Key für die Authentisierung am RADIUS-Server oder der verwendete Schlüssel (beispielsweise für WPA2-Personal) auslesen. Mit diesen Informationen kann dann unberechtigt auf das WLAN zugegriffen werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.2.1 *WLAN-Betrieb* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Planende, Haustechnik

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.2.1.A1 Festlegung einer Strategie für den Einsatz von WLANs (B)

Bevor in einer Institution WLANs eingesetzt werden, MUSS festgelegt sein, welche generelle Strategie die Institution im Hinblick auf die Kommunikation über WLANs plant. Insbesondere MUSS geklärt und festgelegt werden, in welchen Organisationseinheiten, für welche Anwendungen und zu welchem Zweck WLANs eingesetzt und welche Informationen darüber übertragen werden dürfen. Ebenso MUSS der Abdeckungsbereich des WLAN festgelegt werden.

Außerdem MUSS schon in der Planungsphase festgelegt sein, wer für die Administration der unterschiedlichen WLAN-Komponenten zuständig ist, welche Schnittstellen es zwischen den am Betrieb beteiligten Verantwortlichen gibt und wann welche Informationen zwischen den Zuständigen ausgetauscht werden müssen.

NET.2.1.A2 Auswahl eines geeigneten WLAN-Standards (B) [Planende]

Im Rahmen der WLAN-Planung MUSS zuerst ermittelt werden, welche der von der Institution betriebenen Geräte (z. B. Mikrowellengeräte, Bluetooth-Geräte) in das ISM-Band bei 2,4 GHz sowie in das 5 GHz-Band abstrahlen.

Außerdem MÜSSEN die vorhandenen Sicherheitsmechanismen der einzelnen WLAN-Standards gegeneinander abgewogen werden. Generell MUSS sichergestellt sein, dass nur als allgemein sicher anerkannte Verfahren zur Authentisierung und Verschlüsselung eingesetzt werden. Die Entscheidungsgründe MÜSSEN dokumentiert werden.

Geräte, die von anerkannt sicheren Verfahren auf unsichere zurückgreifen müssen, DÜRFEN NICHT mehr eingesetzt werden.

NET.2.1.A3 Auswahl geeigneter Kryptoverfahren für WLAN (B) [Planende]

Die Kommunikation über die Luftschnittstelle MUSS komplett kryptografisch abgesichert werden. Kryptografische Verfahren, die unsicherer als WPA2 sind, DÜRFEN NICHT mehr eingesetzt werden.

Wird WPA2 mit Pre-Shared Keys (WPA2-PSK) verwendet, dann MUSS ein komplexer Schlüssel mit einer Mindestlänge von 20 Zeichen verwendet werden.

NET.2.1.A4 Geeignete Aufstellung von Access Points (B) [Haustechnik]

Access Points MÜSSEN zugriffs- und diebstahlsicher montiert werden. Wenn sie aufgestellt werden, MÜSSEN die erforderlichen Bereiche ausreichend abgedeckt werden. Darüber hinaus MUSS darauf geachtet werden, dass sich die Funkwellen in Bereichen, die nicht durch das WLAN versorgt werden sollen, möglichst nicht ausbreiten. Außeninstallationen MÜSSEN vor Witterungseinflüssen und elektrischen Entladungen geeignet geschützt werden.

NET.2.1.A5 Sichere Basis-Konfiguration der Access Points (B)

Access Points DÜRFEN NICHT in der Konfiguration des Auslieferungszustandes verwendet werden. Voreingestellte SSIDs (Service Set Identifiers), Zugangskennwörter oder kryptografische Schlüssel MÜSSEN vor dem produktiven Einsatz geändert werden. Außerdem MÜSSEN unsichere Administrationszugänge abgeschaltet werden. Access Points DÜRFEN NUR über eine geeignet verschlüsselte Verbindung administriert werden.

NET.2.1.A6 Sichere Konfiguration der WLAN-Infrastruktur (B)

Es MUSS sichergestellt sein, dass mittels der WLAN-Kommunikation keine Sicherheitszonen gekoppelt werden und hierdurch etablierte Schutzmaßnahmen umgangen werden.

NET.2.1.A7 Aufbau eines Distribution Systems (B) [Planende]

Bevor ein kabelgebundenes Distribution System aufgebaut wird, MUSS prinzipiell entschieden werden, ob physisch oder logisch durch VLANs auf den Access Switches des kabelbasierten LANs getrennt wird.

NET.2.1.A8 Verhaltensregeln bei WLAN-Sicherheitsvorfällen (B)

Bei einem Sicherheitsvorfall MUSS der IT-Betrieb passende Gegenmaßnahmen einleiten:

- Am Übergabepunkt der WLAN-Kommunikation ins interne LAN SOLLTE bei einem Angriff auf das WLAN die Kommunikation selektiv pro SSID, Access Point oder sogar für die komplette WLAN-Infrastruktur gesperrt werden.
- Wurden Access Points gestohlen, MÜSSEN festgelegte Sicherheitsmaßnahmen umgesetzt werden, damit der Access Point oder hierauf abgespeicherte Informationen nicht missbraucht werden können.
- Wurden WLAN-Clients entwendet und wird eine zertifikatsbasierte Authentisierung verwendet, MÜSSEN die Client-Zertifikate gesperrt werden.

Es MUSS ausgeschlossen werden, dass entwendete Geräte unberechtigt verwendet werden, um auf das Netz der Institution zuzugreifen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.2.1.A9 Sichere Anbindung von WLANs an ein LAN (S) [Planende]

Werden WLANs an ein LAN angebunden, SOLLTE der Übergang zwischen WLANs und LAN abgesichert werden, beispielsweise durch einen Paketfilter. Der Access Point SOLLTE unter Berücksichtigung der Anforderung NET.2.1.A7 *Aufbau eines Distribution Systems* eingebunden sein.

NET.2.1.A10 Erstellung einer Sicherheitsrichtlinie für den Betrieb von WLANs (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die wesentlichen Kernaspekte für einen sicheren Einsatz von WLANs konkretisiert werden. Die Richtlinie SOLLTE allen Verantwortlichen bekannt sein, die an Aufbau und Betrieb von WLANs beteiligt sind. Sie SOLLTE zudem Grundlage für ihre Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Werden die Inhalte der Richtlinie nicht umgesetzt, MUSS geeignet reagiert werden. Die Ergebnisse SOLLTEN geeignet dokumentiert werden.

NET.2.1.A11 Geeignete Auswahl von WLAN-Komponenten (S)

Anhand der Ergebnisse der Planungsphase SOLLTE eine Anforderungsliste erstellt werden, mithilfe derer die am Markt erhältlichen Produkte bewertet werden können. Werden WLAN-Komponenten beschafft, SOLLTE neben Sicherheit auch auf Datenschutz und Kompatibilität der WLAN-Komponenten untereinander geachtet werden.

NET.2.1.A12 Einsatz einer geeigneten WLAN-Management-Lösung (S)

Eine zentrale Managementlösung SOLLTE eingesetzt werden. Der Leistungsumfang der eingesetzten Lösung SOLLTE im Einklang mit den Anforderungen der WLAN-Strategie sein.

NET.2.1.A13 Regelmäßige Sicherheitschecks in WLANs (S)

WLANs SOLLTEN regelmäßig daraufhin überprüft werden, ob eventuell Sicherheitslücken existieren. Zusätzlich SOLLTE regelmäßig nach unbefugt installierten Access Points innerhalb der bereitgestellten WLANs gesucht werden. Weiterhin SOLLTEN die Performance und Abdeckung gemessen werden. Die Ergebnisse von Sicherheitschecks SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTEN untersucht werden.

NET.2.1.A14 Regelmäßige Audits der WLAN-Komponenten (S)

Bei allen Komponenten der WLAN-Infrastruktur SOLLTE regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt sind. Außerdem SOLLTE überprüft werden ob alle Komponenten korrekt konfiguriert

sind. Öffentlich aufgestellte Access Points SOLLTEN regelmäßig stichprobenartig daraufhin geprüft werden, ob es gewaltsame Öffnungs- oder Manipulationsversuche gab. Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTEN untersucht werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.2.1.A15 Verwendung eines VPN zur Absicherung von WLANs (H)

Es SOLLTE ein VPN eingesetzt werden, um die Kommunikation über die WLAN-Infrastruktur zusätzlich abzusichern.

NET.2.1.A16 Zusätzliche Absicherung bei der Anbindung von WLANs an ein LAN (H)

Wird eine WLAN-Infrastruktur an ein LAN angebunden, SOLLTE der Übergang zwischen WLANs und LAN entsprechend des höheren Schutzbedarfs zusätzlich abgesichert werden.

NET.2.1.A17 Absicherung der Kommunikation zwischen Access Points (H)

Die Kommunikation zwischen den Access Points über die Funkschnittstelle und das LAN SOLLTE verschlüsselt erfolgen.

NET.2.1.A18 Einsatz von Wireless Intrusion Detection/Wireless Intrusion Prevention Systemen (H)

Es SOLLTEN Wireless Intrusion Detection Systeme bzw. Wireless Intrusion Prevention Systeme eingesetzt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld WLAN veröffentlicht:

- BSI-Standard zur Internet-Sicherheit (ISi-Reihe): Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

Das National Institute of Standards and Technology (NIST) hat folgende weiterführende Dokumente zum Themenfeld WLAN veröffentlicht:

- NIST Special Publication 800-153 „Guidelines for Securing Wireless Local Area Network (WLANs)“
- NIST Special Publication 800-97 „Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11“

Bundesamt
für Sicherheit in der
Informationstechnik

NET.2.2 WLAN-Nutzung

1. Beschreibung

1.1. Einleitung

Über Wireless LANs (WLANs) können drahtlose lokale Netze aufgebaut oder bestehende drahtgebundene Netze erweitert werden. Bis heute basieren fast alle am Markt verfügbaren WLAN-Komponenten auf dem Standard IEEE 802.11 und seinen Ergänzungen. Eine besondere Rolle nimmt dabei das Firmenkonsortium „Wi-Fi Alliance" ein, das basierend auf dem Standard IEEE 802.11 mit „Wi-Fi" einen Industriestandard geschaffen hat. Dabei bestätigt die Wi-Fi Alliance mit dem Wi-Fi-Gütesiegel, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat.

WLANs bieten einen Gewinn an Komfort und Mobilität. Jedoch birgt die Nutzung auch zusätzliches Gefährdungspotenzial für die Sicherheit der Informationen, da drahtlos kommuniziert wird. Daher ist es wichtig, dass neben dem IT-Betrieb auch die Benutzenden für die möglichen Gefahren sensibilisiert werden, die entstehen können, wenn WLANs unsachgemäß verwendet werden. So müssen die Benutzenden über die erforderlichen Kenntnisse verfügen, um Sicherheitsmaßnahmen richtig verstehen und anwenden zu können. Insbesondere müssen sie wissen, was von ihnen in Hinblick auf Informationssicherheit erwartet wird und wie sie in bestimmten Situationen reagieren sollten, wenn sie WLANs nutzen.

1.2. Zielsetzung

In diesem Baustein soll aufgezeigt werden, wie WLANs sicher genutzt werden können.

1.3. Abgrenzung und Modellierung

Der Baustein NET.2.2 *WLAN-Nutzung* ist auf alle IT-Systeme (WLAN-Clients) anzuwenden, die WLANs nutzen.

Der Baustein enthält grundsätzliche Anforderungen, die bei der Nutzung von WLANs zu beachten und zu erfüllen sind, um den spezifischen Gefährdungen entgegenwirken zu können. Anforderungen, mit deren Hilfe WLANs sicher betrieben werden können, sind dagegen nicht Gegenstand dieses Bausteins, sondern sind im Baustein NET.2.1 *WLAN-Betrieb* beschrieben. Darüber hinaus geht der Baustein nicht auf allgemeine Aspekte von Clients ein. Solche Aspekte werden im Baustein SYS2.1 *Allgemeiner Client* sowie in den betriebssystemspezifischen Bausteinen der Schicht SYS *IT-Systeme* behandelt. Der Baustein NET.2.2 *WLAN-Nutzung* sollte grundsätzlich mit berücksichtigt werden, wenn die Bausteine ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* und DER.2.1 *Behandlung von Sicherheitsvorfällen* umgesetzt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.2.2 *WLAN-Nutzung* von besonderer Bedeutung.

2.1. Unzureichende Kenntnis über Regelungen

Kennen die Benutzenden die Regelungen für den korrekten Umgang mit WLANs nicht oder nicht gut genug, können sie sich auch nicht daran halten. Werden Clients zum Beispiel gedankenlos mit fremden drahtlosen Netzen verbunden, können darüber unverschlüsselt übertragenen Informationen abgehört werden. Außerdem können durch den Betreibenden des drahtlosen Netzes Informationen über die Benutzenden wie zum Beispiel besuchte Webseiten, gesammelt werden.

2.2. Nichtbeachtung von Sicherheitsmaßnahmen

Durch Nachlässigkeit und fehlende Kontrollen kommt es immer wieder vor, dass Personen die ihnen empfohlenen oder angeordneten Sicherheitsmaßnahmen nicht oder nur teilweise umsetzen. Wird beispielsweise ein WLAN-Client im Ad-hoc-Modus genutzt, obwohl dies in der Nutzungsrichtlinie ausdrücklich verboten ist, kann ein anderer Client direkt mit dem WLAN-Client kommunizieren. So kann er z. B. unberechtigt auf vertrauliche Dokumente zugreifen, die eventuell auf dem Client freigegeben sind.

2.3. Abhören der WLAN-Kommunikation

Da es sich bei Funk um ein Medium handelt, das sich mehrere Benutzende teilen können („Shared Medium"), können die über WLANs übertragenen Daten problemlos mitgehört und aufgezeichnet werden. Werden die Daten nicht oder nur unzureichend verschlüsselt, können die übertragenen Nutzdaten leicht mitgelesen werden. Zudem überschreiten Funknetze bzw. die ausgesendeten Funkwellen nicht selten die Grenzen der genutzten Räumlichkeiten. So werden Daten auch noch in Bereiche ausgestrahlt, die nicht von den Benutzenden oder der Institution kontrolliert und gesichert werden können.

2.4. Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation

Bei WLANs auf Basis von IEEE 802.11 wird die MAC-Adresse einer WLAN-Karte bei jeder Datenübertragung mit versendet. Da sie unverschlüsselt übertragen wird, können Bewegungsprofile über mobile Benutzende erstellt werden, z. B. wenn diese sich in öffentliche Hotspots einbuchen.

2.5. Vortäuschung eines gültigen Access Points (Rogue Access Point)

Angreifende können sich als Teil der WLAN-Infrastruktur ausgeben, indem sie einen eigenen Access Point mit einem geeignet gewählten WLAN-Namen (SSID) in der Nähe eines WLAN-Clients installieren. Dieser vorgetäuschte Access Point wird als „Rogue Access Point" bezeichnet. Bietet dieser dem WLAN-Client eine stärkere Sendeleistung als der echte Access Point, wird der Client diesen als Basisstation nutzen, falls diese sich nicht gegenseitig authentisieren. Zusätzlich könnte auch der echte Access Point durch einen Denial-of-Service-Angriff ausgeschaltet werden. Die Benutzenden melden sich an einem Netz an, das nur vorgibt, das Zielnetz zu sein. Dadurch ist es den Angreifenden möglich, die Kommunikation abzuhören. Auch durch Poisoning- oder Spoofing-Methoden können Angreifende eine falsche Identität vortäuschen bzw. den Netzverkehr zu ihren IT-Systemen umlenken. So können sie die Kommunikation belauschen und kontrollieren. Besonders in öffentlichen Funknetzen (sogenannten Hotspots) ist ein Rogue Access Point ein beliebtes Angriffsmittel.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.2.2 *WLAN-Nutzung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Benutzende
Weitere Zuständigkeiten	IT-Betrieb, Vorgesetzte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.2.2.A1 Erstellung einer Nutzungsrichtlinie für WLAN (B) [IT-Betrieb]

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MÜSSEN die wesentlichen Kernaspekte für eine sichere WLAN-Nutzung in einer WLAN-Nutzungsrichtlinie konkretisiert werden. In einer solchen Nutzungsrichtlinie MÜSSEN die Besonderheiten bei der WLAN-Nutzung beschrieben sein, z. B. ob, wie und mit welchen Geräten Hotspots genutzt werden dürfen.

Die Richtlinie MUSS Angaben dazu enthalten, welche Daten im WLAN genutzt und übertragen werden dürfen und welche nicht.

Es MUSS beschrieben sein, wie mit clientseitigen Sicherheitslösungen umzugehen ist. Die Nutzungsrichtlinie MUSS ein klares Verbot enthalten, ungenehmigte Access Points an das Netz der Institution anzuschließen. Außerdem MUSS in der Richtlinie darauf hingewiesen werden, dass die WLAN-Schnittstelle deaktiviert werden muss, wenn sie über einen längeren Zeitraum nicht genutzt wird.

Es MUSS regelmäßig überprüft werden, ob die in der Richtlinie geforderten Inhalte richtig umgesetzt werden. Ist dies nicht der Fall, MUSS geeignet reagiert werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

NET.2.2.A2 Sensibilisierung und Schulung der WLAN-Benutzenden (B) [Vorgesetzte, IT-Betrieb]

Die Benutzenden von WLAN-Komponenten, vornehmlich von WLAN-Clients, MÜSSEN sensibilisiert und zu den in der Nutzungsrichtlinie aufgeführten Maßnahmen geschult werden. Hierfür MÜSSEN geeignete Schulungsinhalte identifiziert und festgelegt werden. Den Benutzenden MUSS genau erläutert werden, was die WLAN-spezifischen Sicherheitseinstellungen bedeuten und warum sie wichtig sind. Außerdem MÜSSEN die Benutzenden auf die Gefahren hingewiesen werden, die drohen, wenn diese Sicherheitseinstellungen umgangen oder deaktiviert werden.

Die Schulungsinhalte MÜSSEN immer entsprechend den jeweiligen Einsatzszenarien angepasst werden. Neben der reinen Schulung zu WLAN-Sicherheitsmechanismen MÜSSEN den Benutzenden jedoch auch die WLAN-Sicherheitsrichtlinie ihrer Institution und die darin enthaltenen Maßnahmen vorgestellt werden. Ebenso MÜSSEN die Benutzenden für die möglichen Gefahren sensibilisiert werden, die von fremden WLANs ausgehen.

NET.2.2.A3 Absicherung der WLAN-Nutzung an Hotspots (B) [IT-Betrieb]

Dürfen Hotspots genutzt werden, MUSS Folgendes umgesetzt werden:

- Jede(r) Benutzende eines Hotspots MUSS seine oder ihre Sicherheitsanforderungen kennen und danach entscheiden, ob und unter welchen Bedingungen ihm oder ihr die Nutzung des Hotspots erlaubt ist.
- Werden Hotspots genutzt, dann SOLLTE sichergestellt werden, dass die Verbindung zwischen Hotspot-Access Point und IT-Systemen der Benutzenden nach dem Stand der Technik kryptografisch abgesichert wird.
- WLANs, die nur sporadisch genutzt werden, SOLLTEN von den Benutzenden aus der Historie gelöscht werden.
- Die automatische Anmeldung an WLANs SOLLTE deaktiviert werden.
- Wenn möglich, SOLLTEN separate Konten mit einer sicheren Grundkonfiguration und restriktiven Berechtigungen verwendet werden.
- Es SOLLTE sichergestellt sein, dass sich keine Benutzenden mit administrativen Berechtigungen von ihren Clients aus an externen WLANs anmelden können.
- Sensible Daten DÜRFEN NUR übertragen werden, wenn allen notwendigen Sicherheitsmaßnahmen auf den Clients, vor allem eine geeignete Verschlüsselung, aktiviert sind.
- Wird die WLAN-Schnittstelle über einen längeren Zeitraum nicht genutzt, MUSS diese deaktiviert werden.
- Über öffentlich zugängliche WLANs DÜRFEN die Benutzenden NUR über ein Virtual Private Network (VPN) auf interne Ressourcen der Institution zugreifen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.2.2.A4 Verhaltensregeln bei WLAN-Sicherheitsvorfällen (S)

Bei WLAN-Sicherheitsvorfällen SOLLTEN die Benutzenden Folgendes umsetzen:

- Sie SOLLTEN ihre Arbeitsergebnisse sichern.
- Sie SOLLTEN den WLAN-Zugriff beenden und die WLAN-Schnittstelle ihres Clients deaktivieren.
- Fehlermeldungen und Abweichungen SOLLTEN durch sie genau dokumentiert werden. Ebenso SOLLTEN sie dokumentieren, was sie gemacht haben, bevor bzw. während der Sicherheitsvorfall eingetreten ist.
- Sie SOLLTEN über eine geeignete Eskalationsstufe (z. B. User Help Desk) den IT-Betrieb benachrichtigen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld WLAN veröffentlicht:

- BSI-Standard zur Internet-Sicherheit (ISi-Reihe): Sichere Anbindung von lokalen Netzen an das Internet (Isi-LANA)
- Das National Institute of Standards and Technology (NIST) hat folgende weiterführende Dokumente zum Themenfeld WLAN veröffentlicht:
  - NIST Special Publication 800-153 „Guidelines for Securing Wireless Local Area Network (WLANs)“
  - NIST Special Publication 800-97 „Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11“

Bundesamt
für Sicherheit in der
Informationstechnik

NET.3.1 Router und Switches

1. Beschreibung

1.1. Einleitung

Router und Switches bilden das Rückgrat heutiger Datennetze. Ein Ausfall eines oder mehrerer dieser Geräte kann zum kompletten Stillstand der gesamten IT-Infrastruktur führen. Sie müssen daher besonders abgesichert werden.

Router arbeiten auf der OSI-Schicht 3 (Netzschicht) und vermitteln Datenpakete anhand der Ziel-IP-Adresse im IP-Header. Router sind in der Lage, Netze mit unterschiedlichen Topographien zu verbinden. Sie werden verwendet, um lokale Netze zu segmentieren oder um lokale Netze über Weitverkehrsnetze zu verbinden. Ein Router identifiziert eine geeignete Verbindung zwischen dem Quellsystem bzw. Quellnetz und dem Zielsystem bzw. Zielnetz. In den meisten Fällen geschieht dies, indem er die Datenpakete an den nächsten Router weitergibt.

Switches arbeiteten ursprünglich auf der OSI-Schicht 2, mittlerweile sind sie jedoch mit unterschiedlichen Funktionen erhältlich. Firmen kennzeichnen die Geräte meist mit dem OSI-Layer, der unterstützt wird. Dadurch entstanden die Begriffe Layer-2-, Layer-3- und Layer-4-Switch, wobei es sich bei Layer-3- und Layer-4-Switches eigentlich funktional bereits um Router handelt. Die ursprünglich unterschiedlichen Funktionen von Switches und Routern werden somit heute oft auf einem Gerät vereint.

1.2. Zielsetzung

Der Baustein beschreibt, wie Router und Switches sicher eingesetzt werden können.

1.3. Abgrenzung und Modellierung

Der Baustein NET.3.1 *Router und Switches* ist auf jeden im Informationsverbund eingesetzten Router und Switch anzuwenden.

Es ist eine große Auswahl von unterschiedlichen Routern und Switches von verschiedenen Firmen am Markt verfügbar. Der Baustein beschreibt keine spezifischen Anforderungen für bestimmte Produkte. Er ist so weit wie möglich unabhängig von einzelnen Produkten gehalten.

Durch die Verschmelzung der Funktionen von Routern und Switches kann der Großteil der Anforderungen sowohl auf Router als auch auf Switches angewendet werden. Der vorliegende Baustein unterscheidet hier weitgehend nicht zwischen den Gerätearten.

Heute bieten auch nahezu alle Betriebssysteme von Servern und auch Clients eine Routing-Funktionalität an. Dieser Baustein benennt keine Anforderungen für aktivierte Routing-Funktionen in Betriebssystemen von Servern und Clients.

Darüber hinaus werden Aspekte der infrastrukturellen Sicherheit nicht in diesem Baustein aufgeführt, wie z. B. die geeignete Aufstellung, Stromversorgung oder Verkabelung. Sicherheitsanforderungen zu diesen Themen finden sich in den jeweiligen Bausteinen der Schicht INF *Infrastruktur*.

Der vorliegende Baustein beschreibt keine Anforderungen, wie virtuelle Router und Switches abgesichert werden können. Ebenso wird nicht auf eventuell vorhandene Firewall-Funktionen von Routern und Switches eingegangen. Dazu muss zusätzlich der Baustein NET.3.2 *Firewall* umgesetzt werden. Einige Aspekte des Netzdesigns und -managements sind auch für den Einsatz von Routern und Switches von Bedeutung und werden im Rahmen der entsprechenden Anforderungen erwähnt. Weitere Informationen für den Aufbau, das Design und das Management eines Netzes sind in den Bausteinen NET.1.1 *Netzarchitektur und -design* bzw. NET.1.2 *Netzmanagement* zu finden.

Router und Switches sollten grundsätzlich mit berücksichtigt werden, wenn die Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement*, CON.3 *Datensicherungskonzept* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* umgesetzt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.3.1 *Router und Switches* von besonderer Bedeutung.

2.1. Distributed Denial of Service (DDoS)

Bei einem DDoS-Angriff auf ein geschütztes Netz, beispielsweise per TCP SYN Flooding oder UDP Packet Storm, kann aufgrund der vielen Netzverbindungen, die verarbeitet werden müssen, der Router ausfallen. Das kann dazu führen, dass bestimmte Dienste im Local Area Network (LAN) nicht mehr verfügbar sind oder das gesamte LAN ausfällt.

2.2. Manipulation

Gelingt es Angreifenden, unberechtigt auf einen Router oder Switch zuzugreifen, können sie die Geräte neu konfigurieren oder auch zusätzliche Dienste starten. Die Konfiguration lässt sich beispielsweise so verändern, dass Dienste, Clients oder ganze Netzsegmente geblockt werden. Gleichzeitig kann so Netzverkehr am Switch abgefangen, gelesen oder manipuliert werden.

2.3. Fehlerhafte Konfiguration eines Routers oder Switches

Router und Switches werden mit einer Standardkonfiguration ausgeliefert, in der viele Dienste aktiviert sind. Auch verraten Login-Banner beispielsweise die Modell- und Versionsnummer des Gerätes. Werden Router und Switches mit unsicheren Werkseinstellungen produktiv eingesetzt, kann einfacher unberechtigt auf sie zugegriffen werden. Im schlimmsten Fall sind dadurch interne Dienste für Angreifende erreichbar.

2.4. Fehlerhafte Planung und Konzeption

Viele Institutionen planen und konzipieren den Einsatz von Routern und Switches fehlerhaft. So werden unter anderem Geräte beschafft, die nicht ausreichend dimensioniert sind, z. B. hinsichtlich der Port-Anzahl oder der Leistung. In der Folge kann ein Router oder Switch bereits überlastet sein, wenn er zum ersten Mal eingesetzt wird. Dadurch sind eventuell Dienste oder ganze Netze nicht erreichbar und der Fehler muss aufwendig korrigiert werden.

2.5. Inkompatible aktive Netzkomponenten

Kompatibilitätsprobleme können insbesondere dann entstehen, wenn bestehende Netze um aktive Netzkomponenten anderer Firmen ergänzt oder wenn Netze mit Netzkomponenten unterschiedlicher Firmen betrieben werden. Werden aktive Netzkomponenten mit unterschiedlichen Implementierungen desselben Kommunikationsverfahrens gemeinsam in einem Netz betrieben, können einzelne Teilbereiche des Netzes, bestimmte Dienste oder sogar das gesamte Netz ausfallen.

2.6. MAC-Flooding

Beim MAC-Flooding schicken Angreifende viele Anfragen mit wechselnden Quell-MAC-Adressen an einen Switch. Sobald der Switch dann die Limits der MAC-Adressen, die er speichern kann, erreicht hat, fängt er an, sämtliche Anfragen an alle IT-Systeme im Netz zu schicken. Dadurch können Angreifende den Netzverkehr einsehen.

2.7. Spanning-Tree-Angriffe

Bei Spanning-Tree-Angriffen versenden Angreifende sogenannte Bridge Protocol Data Units (BPDUs) mit dem Ziel, die Switches dazu zu bringen, einen eigenen (bösartigen) Switch als Root Bridge anzusehen. Dadurch wird der Netzverkehr über den Switch der Angreifenden umgeleitet, sodass sie alle über ihn versendeten Informationen mit-

schneiden können. In der Folge können sie DDoS-Attacken initiieren und durch falsche BPDUs das Netz dazu zwingen, die Spanning-Tree-Topologie neu aufzubauen, wodurch das Netz ausfallen kann.

2.8. GARP-Attacken

Bei Gratuitous-ARP (GARP)-Attacken senden Angreifende unaufgeforderte ARP-Antworten an bestimmte Opfer oder an alle IT-Systeme im selben Subnetz. In dieser gefälschten ARP-Antwort tragend die Angreifenden ihre MAC-Adresse als Zuordnung zu einer fremden IP-Adresse ein und bringt das Opfer dazu, seine ARP-Tabelle so zu verändern, dass der Netzverkehr nun zu den Angreifenden, anstatt zum validen Ziel gesendet wird. Dadurch können sie die Kommunikation zwischen den Opfern mitschneiden oder sie manipulieren.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.3.1 *Router und Switches* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.3.1.A1 Sichere Grundkonfiguration eines Routers oder Switches (B)

Bevor ein Router oder Switch eingesetzt wird, MUSS er sicher konfiguriert werden. Alle Konfigurationsänderungen SOLLTEN nachvollziehbar dokumentiert sein. Die Integrität der Konfigurationsdateien MUSS in geeigneter Weise geschützt werden. Bevor Zugangspasswörter abgespeichert werden, MÜSSEN sie mithilfe eines zeitgemäßen kryptografischen Verfahrens abgesichert werden.

Router und Switches MÜSSEN so konfiguriert sein, dass nur zwingend erforderliche Dienste, Protokolle und funktionale Erweiterungen genutzt werden. Nicht benötigte Dienste, Protokolle und funktionale Erweiterungen MÜSSEN deaktiviert oder ganz deinstalliert werden. Ebenfalls MÜSSEN nicht benutzte Schnittstellen auf Routern und Switches deaktiviert werden. Unbenutzte Netzports MÜSSEN nach Möglichkeit deaktiviert oder zumindest einem dafür eingerichteten *Unassigned-VLAN* zugeordnet werden.

Wenn funktionale Erweiterungen benutzt werden, MÜSSEN die Sicherheitsrichtlinien der Institution weiterhin erfüllt sein. Auch SOLLTE begründet und dokumentiert werden, warum solche Erweiterungen eingesetzt werden.

Informationen über den internen Konfigurations- und Betriebszustand MÜSSEN nach außen verborgen werden. Unnötige Auskunftsdienste MÜSSEN deaktiviert werden.

NET.3.1.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.1.A4 Schutz der Administrationsschnittstellen (B)

Alle Administrations- und Managementzugänge der Router und Switches MÜSSEN auf einzelne Quell-IP-Adressen bzw. -Adressbereiche eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht vertrauenswürdigen Netzen heraus nicht direkt auf die Administrationsschnittstellen zugegriffen werden kann.

Um Router und Switches zu administrieren bzw. zu überwachen, SOLLTEN geeignet verschlüsselte Protokolle eingesetzt werden. Sollte dennoch auf unverschlüsselte Protokolle zurückgegriffen werden, MUSS für die Administration ein eigenes Administrationsnetz (Out-of-Band-Management) genutzt werden. Die Managementschnittstellen und die Administrationsverbindungen MÜSSEN durch eine separate Firewall geschützt werden. Für die Schnittstellen MÜSSEN geeignete Zeitbeschränkungen für z. B. Timeouts vorgegeben werden.

Alle für das Management-Interface nicht benötigten Dienste MÜSSEN deaktiviert werden. Verfügt eine Netzkomponente über eine dedizierte Hardwareschnittstelle, MUSS der unberechtigte Zugriff darauf in geeigneter Weise unterbunden werden.

NET.3.1.A5 Schutz vor Fragmentierungsangriffen (B)

Am Router und Layer-3-Switch MÜSSEN Schutzmechanismen aktiviert sein, um IPv4- sowie IPv6-Fragmentierungsangriffe abzuwehren.

NET.3.1.A6 Notfallzugriff auf Router und Switches (B)

Es MUSS für die Administrierenden immer möglich sein, direkt auf Router und Switches zuzugreifen, sodass diese weiterhin lokal administriert werden können, auch wenn das gesamte Netz ausfällt.

NET.3.1.A7 Protokollierung bei Routern und Switches (B)

Ein Router oder Switch MUSS so konfiguriert werden, dass er unter anderem folgende Ereignisse protokolliert:

- Konfigurationsänderungen (möglichst automatisch),
- Reboot,
- Systemfehler,
- Statusänderungen pro Interface, System und Netzsegment sowie
- Login-Fehler

NET.3.1.A8 Regelmäßige Datensicherung (B)

Die Konfigurationsdateien von Routern und Switches MÜSSEN regelmäßig gesichert werden. Die Sicherungskopien MÜSSEN so abgelegt werden, dass im Notfall darauf zugegriffen werden kann.

NET.3.1.A9 Betriebsdokumentationen (B)

Die wichtigsten betrieblichen Aufgaben eines Routers oder Switches MÜSSEN geeignet dokumentiert werden. Es SOLLTEN alle Konfigurationsänderungen sowie sicherheitsrelevante Aufgaben dokumentiert werden. Die Dokumentation SOLLTEN vor unbefugten Zugriffen geschützt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.3.1.A10 Erstellung einer Sicherheitsrichtlinie (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTE eine spezifische Sicherheitsrichtlinie erstellt werden. In der Sicherheitsrichtlinie SOLLTEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie Router und Switches sicher betrieben werden können. Die Richtlinie SOLLTE allen Administrierenden bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den festgelegten Anforderungen